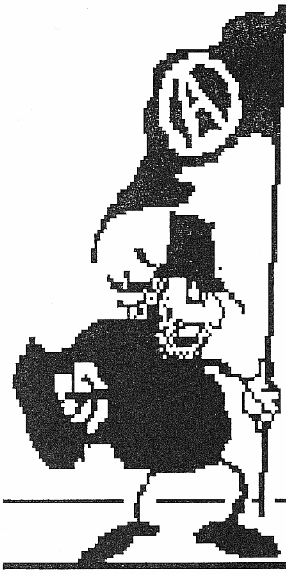



# Ο ΑΝΑΡΧΙΚΟΣ

## ΔΕΛΤΙΟ ΠΛΗΡΟΦΟΡΗΣΗΣ


Η επικαιρότητα του θέματος των υποκλοπών μάς ανάγκασε να καθυστερήσουμε την έκδοση αυτού του τεύχους και να παραλείψουμε την συνηθισμένη μας ύλη.
Θα επανορθώσουμε το συντομώτερο δυνατόν.




ΑΘΗΝΑ, 9 ΜΑΡΤΗ 2006 - τεύχος 278


**Την ώρα που τυπώνεται το σημερινό τεύχος, ο διευθύνων σύμβουλος (καί ήδη «περιφερειακός διευθυντής Βαλκανίων») της Vodafone, ο Γιώργος Κορωνιάς, καταθέτει στην «Επιτροπή Θεσμών και Διαφάνειας της Βουλής» για το «σκάνδαλο των τηλεφωνικών υποκλοπών», το οποίο - ΣΚΑΝΔΑΛΩΔΩΣ - «σκανδαλίζει» τους «πατέρες και τις μητέρες (για να μην ξεχνάμε και την χθεσινή παγκόσμια μέρα - γαϊτανάκι της Γυναίκας) του Έθνους», ΜΟΝΟ ΤΟΝ ΤΕΛΕΥΤΑΙΟ ΜΗΝΑ !!!**

**Λες κι αγνοούσαν αυτό που
Ο ΚΟΣΜΟΣ ΤΟ 'ΧΕΙ ΤΟΥΜΠΑΝΟ
ΚΙ ΑΥΤΟΙ ΚΡΥΦΟ ΚΑΜΑΡΙ !!!**

**Για «του λόγου το αληθές»,
παρουσιάζουμε στο σημερινό μας τεύχος
ΑΠΟΚΛΕΙΣΤΙΚΑ
για τους αναγνώστες του Αναρχικού
το**

**INTERCEPTIONS MANAGEMENT SYSTEM USER MANUAL
- ΕΓΧΕΙΡΙΔΙΟ ΧΡΗΣΤΗ του ΣΥΣΤΗΜΑΤΟΣ ΔΙΑΧΕΙΡΙΣΗΣ ΥΠΟΚΛΟΠΩΝ -
της Ericsson.**

STRICTLY CONFIDENTIAL




# *IMS User Manual*

**STRICTLY CONFIDENTIAL**, δηλαδή **ΑΥΣΤΗΡΩΣ ΕΜΠΙΣΤΕΥΤΙΚΟ**, χαρακτηρίζεται από την **Ericsson** το **IMS 7.1.8 User Manual**, δηλαδή το **Εγχειρίδιο Χρήστη του IMS 7.1.8**...
Όπως μάς πληροφορεί το Εγχειρίδιο, στην Εισαγωγή του 1ου Κεφαλαίου (σελίδα 14 - όλο το Εγχειρίδιο έχει 292 σελίδες), τα αρχικά **IMS σημαίνουν «INTERCEPTION MANAGEMENT SYSTEM», δηλαδή «ΣΥΣΤΗΜΑ ΔΙΑΧΕΙΡΙΣΗΣ ΥΠΟΚΛΟΠΩΝ»** !
Η έκδοση 7.1.8 του συστήματος εκδόθηκε το 2001. Με κάποιες - ελάχιστες - μετατροπές, το IMS εξακολουθεί, πάντως, να χρησιμοποιείται μέχρι σήμερα από τη Ericsson και τις εταιρίες που συνεργάζονται μαζί της, σαν την Vodafone.

Το «Εγχειρίδιο», όπως αναφέρεται σε ένδειξη που εμφανίζεται σε κάποιες σελίδες του, «ετοιμάστηκε από τον Bruce Ashley, εγκρίθηκε από τον Elton Cross» και κυκλοφόρησε «αναθεωρημένο στις 14/3/2001».

| Prepared by | EPA/D/N: Bruce Ashley | Document no. | 1/155 17-CNAP 102 11 Uen | | | |
|---|---|---|---|---|---|---|
| Approved by | EPA/D/N: (Elton Cross) | Revision date | 2001-03-14 | Revision T | | Pages 22 |

*Ο αριθμός των σελίδων (22) είναι ο αριθμός των σελίδων του εισαγωγικού κεφαλαίου του εγχειριδίου. Το αντίτυπο που δημοσιεύτηκε σε αρκετές ιστοσελίδες του διαδικτύου, σε μορφή «pdf» (portable document format, δηλαδή «φορητό έγγραφο» που διαβάζεται από το πρόγραμμα Acrobat της εταιρίας Adobe), όπως είπαμε, έχει συνολικά 292 σελίδες.*

Φυσικά, ο αριθμός των αποδεκτών περιοριζόταν στον στενό κύκλο των «χειριστών του συστήματος», δηλαδή στους «νόμιμους» δράστες των υποκλοπών - υπαλλήλους των εταιριών και των μυστικών υπηρεσιών.

«Νόμιμους;» Θ'αναρρωτηθεί κάποιος (προφανώς από κάποιον άλλο πλανήτη).
«Μα, φυσικά, νόμιμους !».
Οι νόμοι, βλέπετε, επιτρέπουν την παραβίαση του - συνταγματικά κατοχυρωμένου - «απορρήτου των επικοινωνιών», σε «ορισμένες περιπτώσεις» και από «ορισμένους υπευθύνους»...
Η «δημόσια ασφάλεια» και το «εθνικό συμφέρον» αποτελούν τους όρους-κλειδιά. Τί σημαίνουν αυτοί οι όροι; Μα, «φυσικά», την ΑΣΦΑΛΕΙΑ και το ΣΥΜΦΕΡΟΝ των ΜΕΓΑΛΟΚΑΡΧΑΡΙΩΝ (οικονομικών και, δευτερευόντως, πολιτικών), που λυμαίνονται την ζωή των υπολοίπων μορφών ζωής του πλανήτη μας.
Ποιός ερμηνεύει έτσι αυτούς τους όρους; Μα, βέβαια, η μόνη αρχή που έχει το «δικαίωμα» να ερμηνεύει τα πάντα : Η ΚΥΒΕΡΝΗΣΗ ΤΩΝ ΗΝΩΜΕΝΩΝ ΠΟΛΙΤΕΙΩΝ !!!
Ποιός τής δίνει αυτό το «δικαίωμα»; Δεν χρειάζεται μεγάλη σοφία για να απαντηθεί το εύλογο αυτό ερώτημα. Η ΤΕΡΑΣΤΙΑ ΠΟΛΕΜΙΚΗ (και ΟΙΚΟΝΟΜΙΚΗ, σε δεύτερο βαθμό) ΙΣΧΥΣ ΤΩΝ ΗΠΑ τους ΔΙΝΕΙ ΤΟ ΔΙΚΑΙΩΜΑ ΣΤΗΝ ΚΥΒΕΡΝΗΣΗ ΤΟΥΣ ΝΑ ΕΡΜΗΝΕΥΕΙ ΤΑ ΠΑΝΤΑ. Στο μέτρο που οι υπόλοιπες κυβερνήσεις και οι υπόλοιποι λαοί υποτάσσονται σ' αυτή την ισχύ, Η ΟΠΟΙΑ ΕΡΜΗΝΕΙΑ ΠΡΟΕΡΧΕΤΑΙ ΑΠΟ ΤΟ ΚΟΝΓΚΡΕΣΣΟ, ΤΗΝ ΓΕΡΟΥΣΙΑ ή ΤΟΝ ΕΚΑΣΤΟΤΕ ΕΝΟΙΚΟ ΤΟΥ ΛΕΥΚΟΥ ΟΙΚΟΥ ΤΗΣ WASHINGTON, ΕΙΝΑΙ **ΑΥΘΕΝΤΙΚΗ**.
Χωρίζονται, λοιπόν, οι υποκλοπείς των τηλεφωνικών (όπως και των υπολοίπων, π.χ. των ταχυδρομικών) μας επικοινωνιών σε «νόμιμους» και «παράνομους». Η διάκριση δεν είναι, όμως, απλά νομικίστικη. Πέρα από το νομοθετικό και το δικαστικό πεδίο (όπου δημιουργεί σωρεία ολόκληρη προβλημάτων, τα οποία χρειάζονται ευρύτερη και βαθύτερη μελέτη, όχι μόνο από τους νομικούς, αλλά και από κάθε απλό μέλος της κοινωνίας), η διάκριση των υποκλοπέων σε «νόμιμους» και «παράνομους» εισβάλλει και στο πεδίο της επιστήμης, της τεχνολογίας και των εφαρμογών τους στην καθημερινή ζωή.
Ιστορικά, το φαινόμενο των επικοινωνιακών υποκλοπών είναι πανάρχαιο, όπως πανάρχαια είναι και τα μέσα αντιμετώπισής τους και προστασίας των επικοινωνιών, τόσο του δημοσίου, όσο και του ιδιωτικού τομέα : **Κρυπτογραφία** και **στεγανοποίηση** (από την γραφή στο ξυρισμένο κεφάλι του αγγελιαφόρου και στο ξαναξύρισμα του κεφαλιού από τον παραλήπτη του μηνύματος, την σκυτάλη των αρχαίων Ελλήνων, την γραφή με ανεξίτηλο μελάνι σε επιφάνεια που καλυπτόταν με μη-ανεξίτηλο όμοιο χρώμα, την χρήση συνθηματικών όρων, τον κώδικα του Ιουλίου Καίσαρος και τον κώδικα του Vigénθre, μέχρι τα κρυπτογραφικά συστήματα της εποχής των ναπολεοντείων πολέμων, την συνθηματική εμπορική αλληλογραφία των αρχών του 19ου αιώνα, τον κώδικα της Φιλικής Εταιρείας, και μέχρι την κρυπτομηχανή Enigma του Β΄ Παγκ. Πολέμου, τα κρυπτοσυστήματα των τραπεζών και των μεγάλων (και μικρών) επιχειρήσεων, την κρυπτογραφία «δημόσιας κλείδας» ή «public key cryptography», έως το σύστημα των Rivest-Shamir-Adleman, την χρήση εναλασσομένων ραδιοσυχνοτήτων και συσκευών ανάμιξης επικοινωνιακών στοιχείων, δηλαδή των «scramblers», κ.λπ., που εμφανίζονται τις τελευταίες δεκαετίες του 20ου και κυριαρχούν στις μέρες μας), **αντικατασκοπεία** (εντοπισμός κατασκόπων του εχθρού, διοχέτευση παραπλανητικών πληροφοριών, εξουδετέρωση εχθρικών πρακτόρων, χρήση συσκευών που εμποδίζουν την εκπομπή δευτερευόντων σημάτων από τις ηλεκτρονικές μας συσκευές και εξουδετερώνουν τις τεχνικές «Tempest», κ.λπ.), **φυσικό έλεγχο** των επικοινωνιακών εγκαταστάσεων και δικτύων (π.χ. έλεγχο των τηλεφωνικών καλωδίων, των ΚΑΦΑΟ, εντοπισμό κρυμμένων μικροφώνων)...

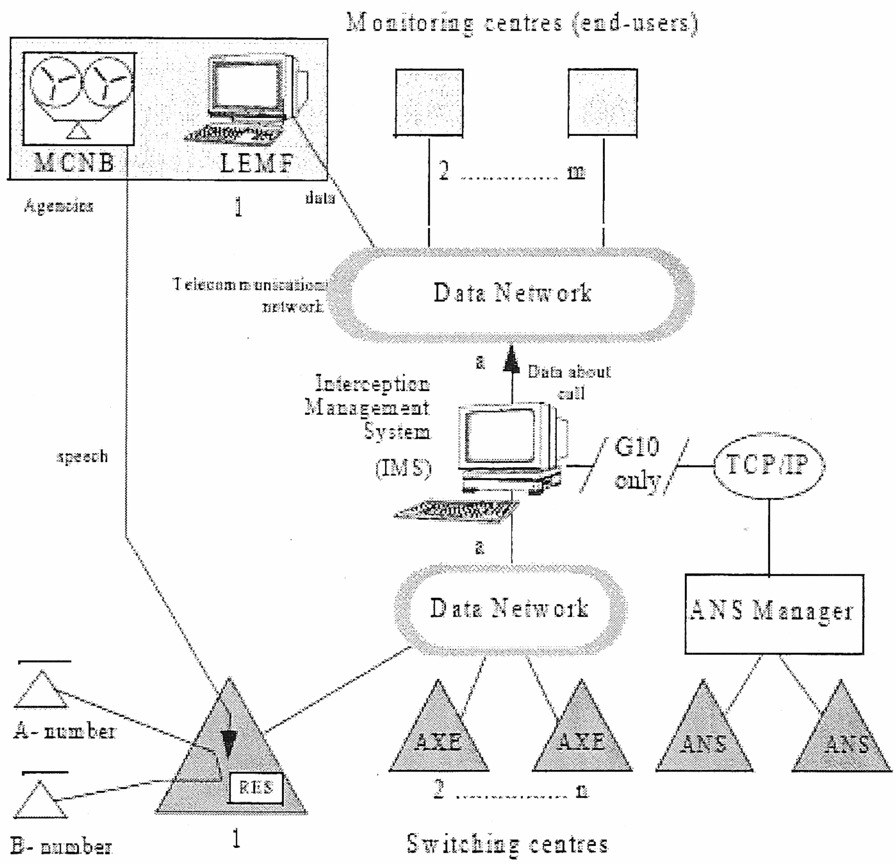
Ας γυρίσουμε, όμως, στην Ericsson και στο IMS.

Ένα λίαν κατατοπιστικό σχεδιάγραμμα, που περιλαμβάνεται στο «Εγχειρίδιο» (σελίδα 16), μάς διαφωτίζει για το τί ακριβώς κάνει ένα «σύστημα υποκλοπών».

CHAPTER 1 Functional Specification of IMS
Overview

STRICTLY CONFIDENTIAL

*Figure 1.1* Telecommunication interception model




## Applicability

IMS supports all network technologies where the RES function is applicable. This document deals with its implementation in:

- Analog Mobile (CMS 88), for monitoring voice calls,
- Digital Mobile (CME 20), for monitoring voice, data and SMS calls,
- PSDN/ISDN, for monitoring voice and data calls, and
- ANS switch, for monitoring voice and data calls (G10).

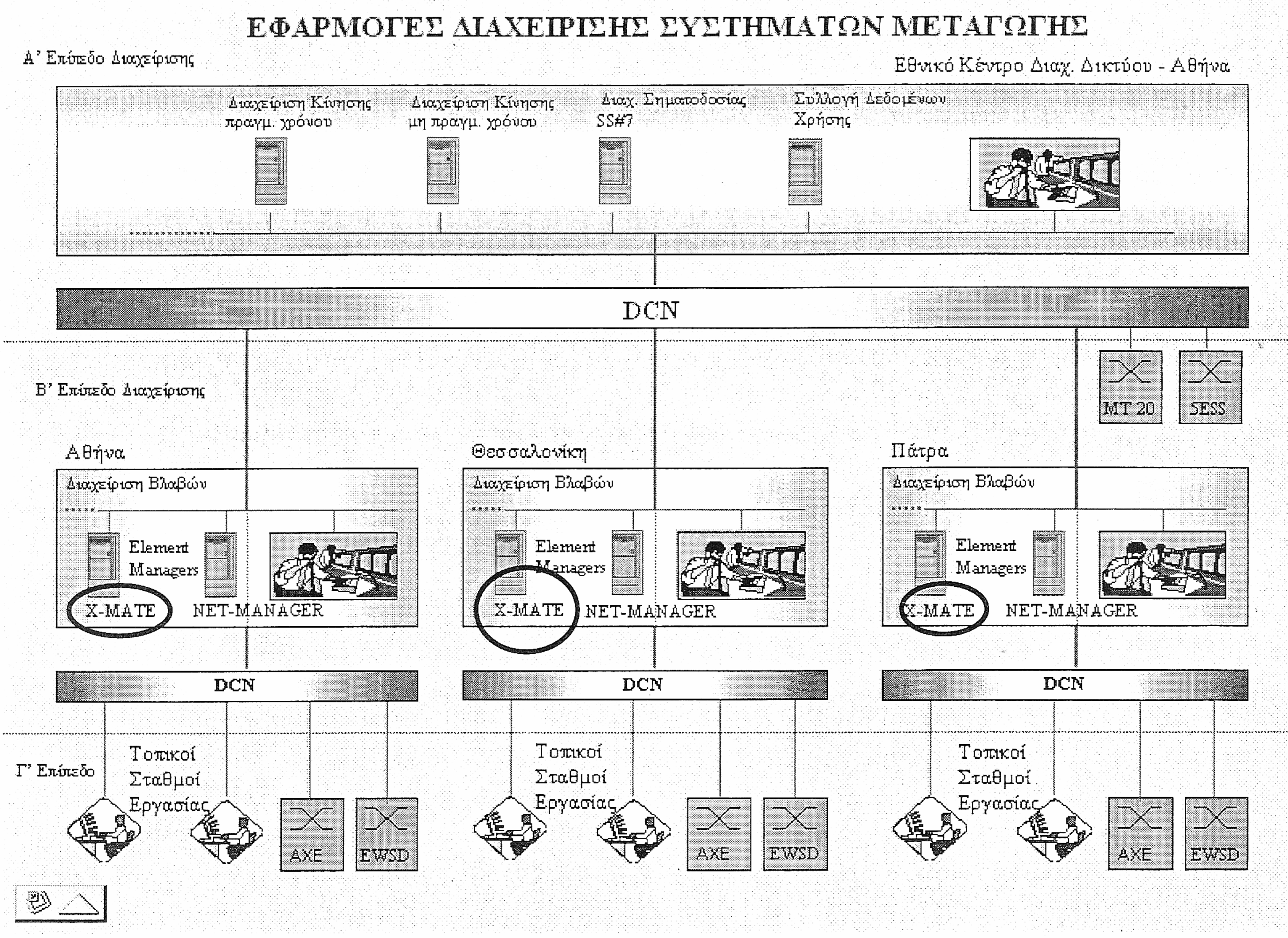
1-4

Αρχίζοντας από κάτω, αριστερά, έχουμε δυο συνδρομητές τηλεφωνίας (απ' τους οποίους ο ένας ή και οι δυο έχουν κινητό τηλέφωνο), τον **A** και τον **B**. Για να επικοινωνήσουν αυτοί οι δυο μεταξύ τους, ακολουθείται η εξής διαδικασία : Ο καλών (A) συνδέεται - μέσω τηλεφωνικού καλωδίου (αν έχει σταθερό) ή ασύρματα (αν έχει κινητό τηλέφωνο) - με κάποιον «κόμβο» (ή «κομβικό κέντρο» - «**switching centre**») της εταιρίας. Ο κόμβος αυτός μπορεί να διαθέτει **AXE** (Automatic Exchange Equipment), δηλαδή «αυτόματο μηχανισμό ανταλλαγής» ή ANS (Access Node Switch), δήλαδή ένα «διακόπτη πρόσβασης σε κάποιον

άλλο κόμβο».
Στο εσωτερικό, λοιπόν, αυτού του «κομβικού κέντρου», ο μηχανισμός διακρίνει αυτόματα αν το περιεχόμενο του μηνύματος είναι **αναλογικό** (φωνή) ή **ψηφιακό** (δεδομένα ηλεκτρονικής μορφής) και, αφού καλέσει τον καλούμενο (B) - είτε καλωδιακά, μέσω των σταθερών γραμμών π.χ. του ΟΤΕ, είτε ασύρματα, μέσω κάποιας κεραίας απ' αυτές που βλέπουμε εγκατεστημένες σε διάφορα σημεία της χώρας - τού μεταβιβάζει την κλήση και στην συνέχεια μεσολαβεί μεταδίδοντας τα στοιχεία της επικοινωνίας από τον καλούντα στον καλούμενο, λειτουργώντας ουσιαστικά με τον ίδιο τρόπο που λειτουργεί κι ένα συμβατικό κέντρο σταθερής (καλωδιακής) τηλεφωνίας, με την διαφορά ότι η μεταβίβαση αυτών των στοιχείων προς και από τους δυο συνδρομητές (ή μόνο τον ένα και το κέντρο της καλωδιακής τηλεφωνίας) γίνεται ασύρματα, στις διεθνώς καθορισμένες ραδιοσυχνότητες των 824 - 849 MHz (μεγακύκλων).
Εκτός, όμως, από τον AXE, στο εσωτερικό του κομβικού κέντρου είναι εγκατεστημένο και ένα **RES** (Remote-control Equipment Subsystem), δηλαδή ένα «εξ' αποστάσεως ελεγχόμενο υποσύστημα του μηχανισμού (υλικού και λογισμικού)» της υποκλοπής. Το RES, είναι, λοιπόν, η καρδιά του συγκεκριμένου συστήματος υποκλοπών. Χωρίς αυτό, κατά το εγχειρίδιο, το IMS είναι άχρηστο.
Το RES διοχετεύει τα εξωτερικά στοιχεία (αριθμούς, στοιχεία κατόχων των τηλεφωνικών συσκευών, ώρα και γεωγραφική θέση των συνδρομητών κατά την διάρκεια της επικοινωνίας κ.α.) και το περιεχόμενο της επικοινωνίας στα «κέντρα παρακολούθησης», δηλαδή στους «τελικούς χρήστες», όπως φαίνεται στο σχεδιάγραμμα : «**monitoring centres/end users ή MC**».
Στην περίπτωση αναλογικού σήματος (ήχου, φωνής), αυτό στέλνεται κατευθείαν στο MC και ηχογραφείται. Στην περίπτωση που το σήμα είναι ψηφιακό, στέλνεται, μέσω του δικτύου δεδομένων (data network) απευθείας (από το AXE) ή μέσω του «πρωτοκόλλου ελέγχου μεταβίβασης/πρωτοκόλλου διαδικτύου» («TCP/IP - Transmission Control Protocol/Internet Protocol» (από τα ANS), σ' έναν υπολογιστή της εταιρίας κινητής τηλεφωνίας, όπου το IMS, το «σύστημα διαχείρισης των υποκλοπών», το προωθεί στα «κέντρα παρακολούθησης». Το **G10** ή «**Corba protocol**» είναι ένα πρωτόκολλο (σύνολο διαδικασιών) επικοινωνίας του υπολογιστή της εταιρίας με τους υπολογιστές των «κέντρων παρακολούθησης».
Το «κέντρο παρακολούθησης», κατά το σχεδιάγραμμα, περιλαμβάνει στην ουσία δυο μονάδες : το **MCNB** (Monitoring Centre Number Bloc) και την **LEMF** (Law Enforcement Monitoring Facility). Το πρώτο, το «Κέντρο Παρακολούθησης με Αριθμό Κλήσης», ενεργοποιείται μέσω του «δημοσίου δικτύου» (δηλαδή μέσω του κλασσικού τηλεφωνικού δικτύου, καλωδιακού ή ασύρματου), χωρίς την μεσολάβηση του IMS (το οποίο, ωστόσο, ελέγχει την «νομιμότητα» των υποκλοπέων και το οποίο μεταβιβάζει στο «κέντρο» τα «εξωτερικά στοιχεία» της επικοινωνίας). Η δεύτερη, η «Αστυνομική Εγκατάσταση Παρακολούθησης» αποτελείται στην ουσία από έναν υπολογιστή, στην οθόνη του οποίου ο χειριστής βλέπει το περιεχόμενο των ψηφιακών μηνυμάτων (e-mail, SMS, κ.λπ.) που ανταλάσσουν οι συνδρομητές Α και Β. Όποτε χρειαστεί, έχει βέβαια την δυνατότητα να «σώσει» τα όσα βλέπει στον σκληρό δίσκο του υπολογιστή του για την περαιτέρω κατεργασία τους (π.χ. αποκρυπτογράφηση, συσχετισμό τους με άλλα μηνύματα, κ.λπ.).
Το πρώτο κεφάλαιο του «Εγχειριδίου» αναλύει λεπτομερειακά τα όσα γράψαμε παραπάνω.

Το δεύτερο κεφάλαιο του «Εγχειριδίου» ασχολείται με την εγκατάσταση του IMS. Δεν θα κουράσουμε τους αναγνώστες με τις πάμπολλες τεχνικές λεπτομέρειες (τις οποίες ομολογούμε ότι δυσκολευόμαστε και να μεταφράσουμε στα ελληνικά).
Περιοριζόμαστε να αναφέρουμε πως προϋπόθεση της εγκατάστασης του IMS είναι η προηγούμενη εγκατάσταση του **XMATE**, ενός λογισμικού προγράμματος που αναπτύχθηκε από την Ericsson Australia και το οποίο χρησιμεύει ως κεντρική πλατφόρμα επικοινωνιών των υπολογιστών της εταιρίας κινητής τηλεφωνίας (εν προκειμένω της Vodafone, αλλά όχι μόνο αυτής).

Μια περιήγηση στο διαδίκτυο μάς αποκαλύπτει ότι το XMATE είναι εγκατεστημένο όχι μόνο στην Vodafone, αλλά και στον ΟΤΕ.

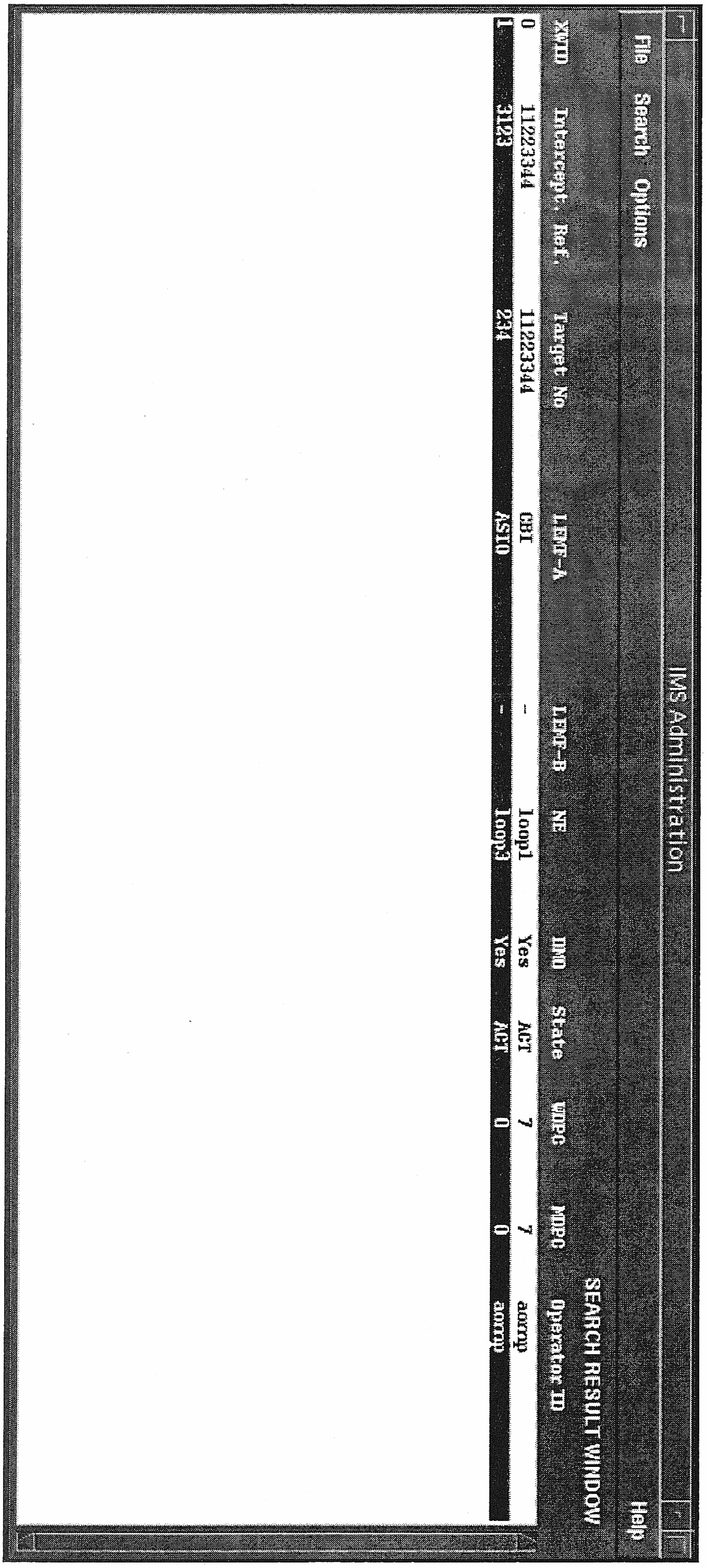



*Σχεδιάγραμμα από πρόσφατη διάλεξη στελέχους του ΟΤΕ για το «Δίκτυο Ψηφιακών Επικοινωνιών» (Digital Communications Network - DCN) του οργανισμού. Οι ομοιότητες με το σχεδιάγραμμα του «Εγχειριδίου» της Ericsson είναι εμφανείς, αν κι εδώ παραλείπονται τα «κέντρα παρακολούθησης».*

Εύλογα, λοιπόν, προκύπτει το ερώτημα : ΑΦΟΥ Ο ΟΤΕ ΕΧΕΙ ΕΓΚΑΤΑΣΤΗΣΕΙ ΤΟ XMATE, ΜΗΠΩΣ ΕΧΕΙ ΕΓΚΑΤΑΣΤΗΣΕΙ ΚΑΙ ΤΟ ΣΥΣΤΗΜΑ ΔΙΑΧΕΙΡΙΣΗΣ ΥΠΟΚΛΟΠΩΝ, ΔΗΛΑΔΗ ΤΟ IMS ;
Και, αν το έχει εγκαταστήσει, ποιός μάς εγγυάται ότι, εκτός από τους «νόμιμους» χρήστες, δεν το χρησιμοποιούν και κάποιοι «παράνομοι» ;

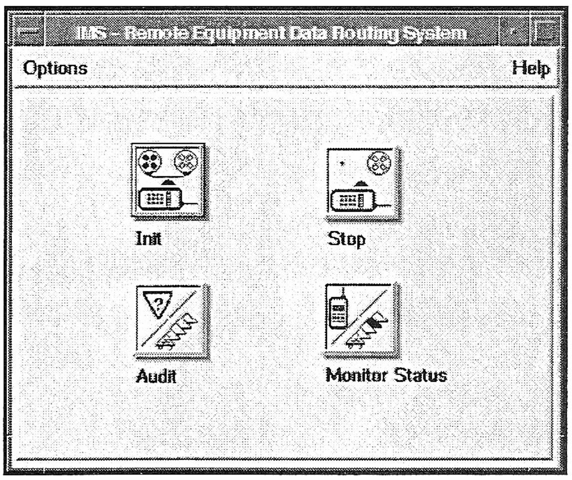
Αφελή ερωτήματα όντων από άλλον πλανήτη... Χωριό που φαίνεται... Ο νοών νοείτω !

Το τρίτο κεφάλαιο του «Εγχειριδίου» περιγράφει τους τρόπους και τις διαδικασίες επαλήθευσης της σωστής εγκατάστασης του IMS. Πρόκειται για μιαν «εικονική» έναρξη, διενέργεια και διακοπή υποκλοπής, ένα «πείραμα» πραγματικής υποκλοπής από κάποιο κινητό τηλέφωνο της εταιρίας, ενεργοποίηση ενός «κέντρου παρακολούθησης», έλεγχο της καλής λειτουργίας του IMS και του XMATE, και «καθάρισμα» του υπολογιστή από όλα τα ίχνη των παραπάνω εργασιών.
Σημαντικό στοιχείο : Το XMATE και το IMS «κάθονται» (βασίζονται) σε λειτουργικό σύστημα UNIX.



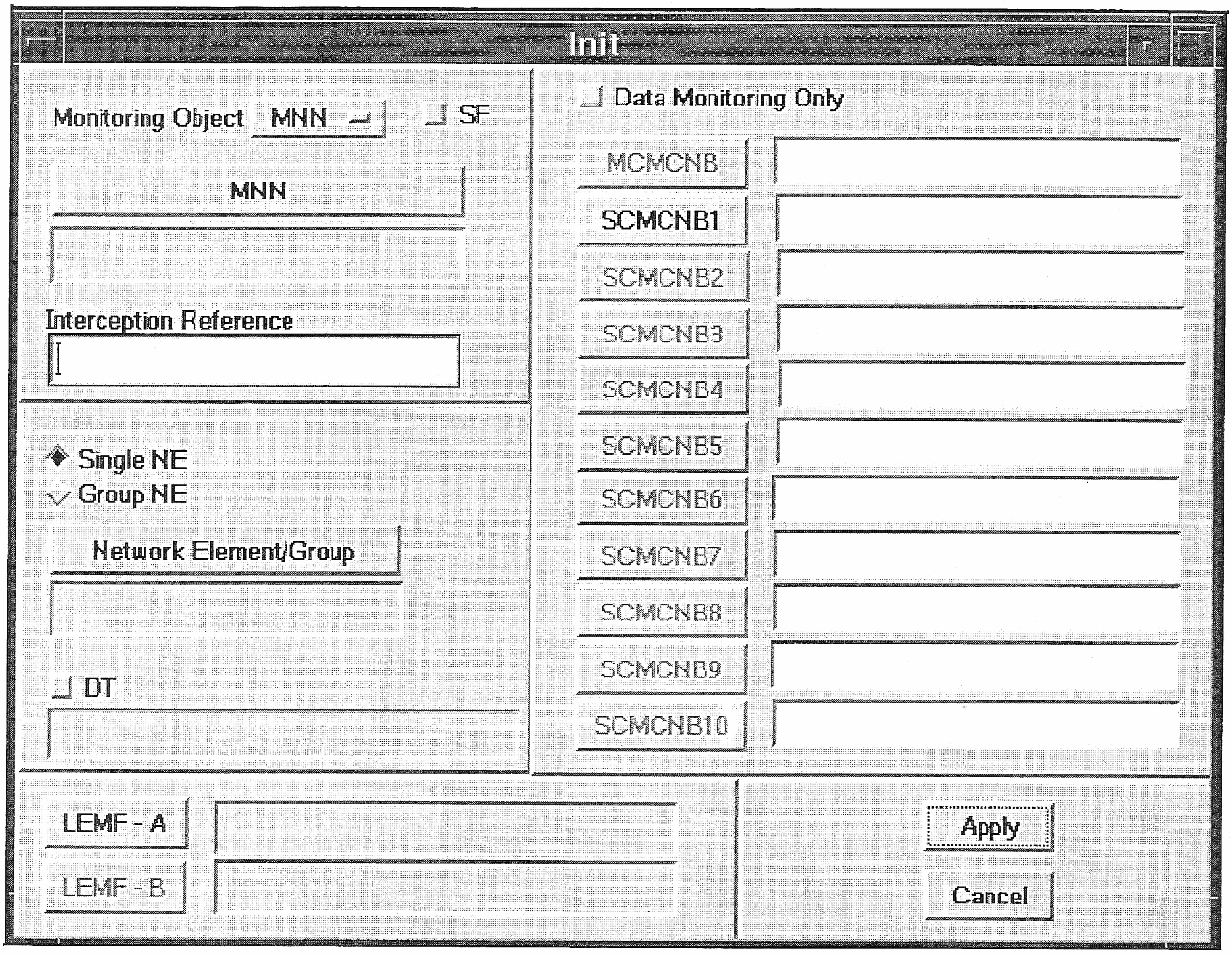

Τα επόμενα δυο κεφάλαια (4 και 5) του «Εγχειριδίου» ασχολούνται με την «διοίκηση» (**administering**) του IMS. Το 4°, με την «διοίκηση της βάσης δεδομένων» (**data base**), δηλαδή με την τήρηση των αρχείων (παραστατικών «νομιμοποίησης» των υποκλοπέων, δικαστικών ενταλμάτων και εισαγγελικών παραγγελιών για την παρακολούθηση των τηλεφωνικών επικοινωνιών των «υπόπτων», της ημερομηνίας και της ώρας της κάθε υποκλοπής...), αλλά και με την τήρηση του αρχείου των «διοικητών», των «διαχειριστών» και των «χειριστών» του συστήματος (**administrators, managers, operators**), των ονοματεπωνύμων, των ηλεκτρονικών τους ταυτοτήτων και των κωδικών πρόσβασης. Το 5° κεφάλαιο, με την διαχείριση της «μεταβίβασης» (**transmission**) των στοιχείων που υποκλέπτονται στα «νόμιμα κέντρα παρακολούθησης».
Ενδιαφέρον παρουσιάζει η αυστηρή ιεράρχηση της πρόσβασης που έχει κάθε εμπλεκόμενος στις υποκλοπές στο αντίστοιχο «επίπεδο ασφαλείας» του IMS και του XMATE.

(Αριστερά, ένα απ' τα «παράθυρα» της «διοίκησης» των υποκλοπών, όπως εμφανίζεται στην οθόνη του υπολογιστή της τηλεφωνικής εταιρίας)

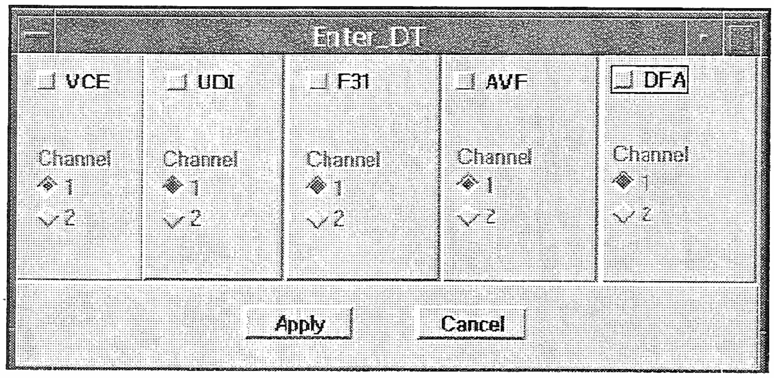


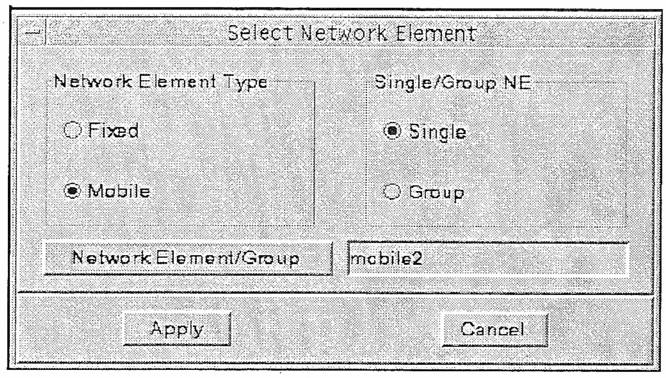

Στο έκτο κεφάλαιο αναλύεται ο τρόπος χειρισμού του συστήματος.

Στην παραπάνω εικόνα εμφανίζεται το «παράθυρο» των τεσσάρων επιλογών του χειριστή : Έναρξη της παρακολούθησης/καταγραφής (**Init**) - Διακοπή (**Stop**) - Ακρόαση/διάβασμο των στοιχείων (**Audit**) - Έλεγχος της κατάστασης (**Monitor Status**).

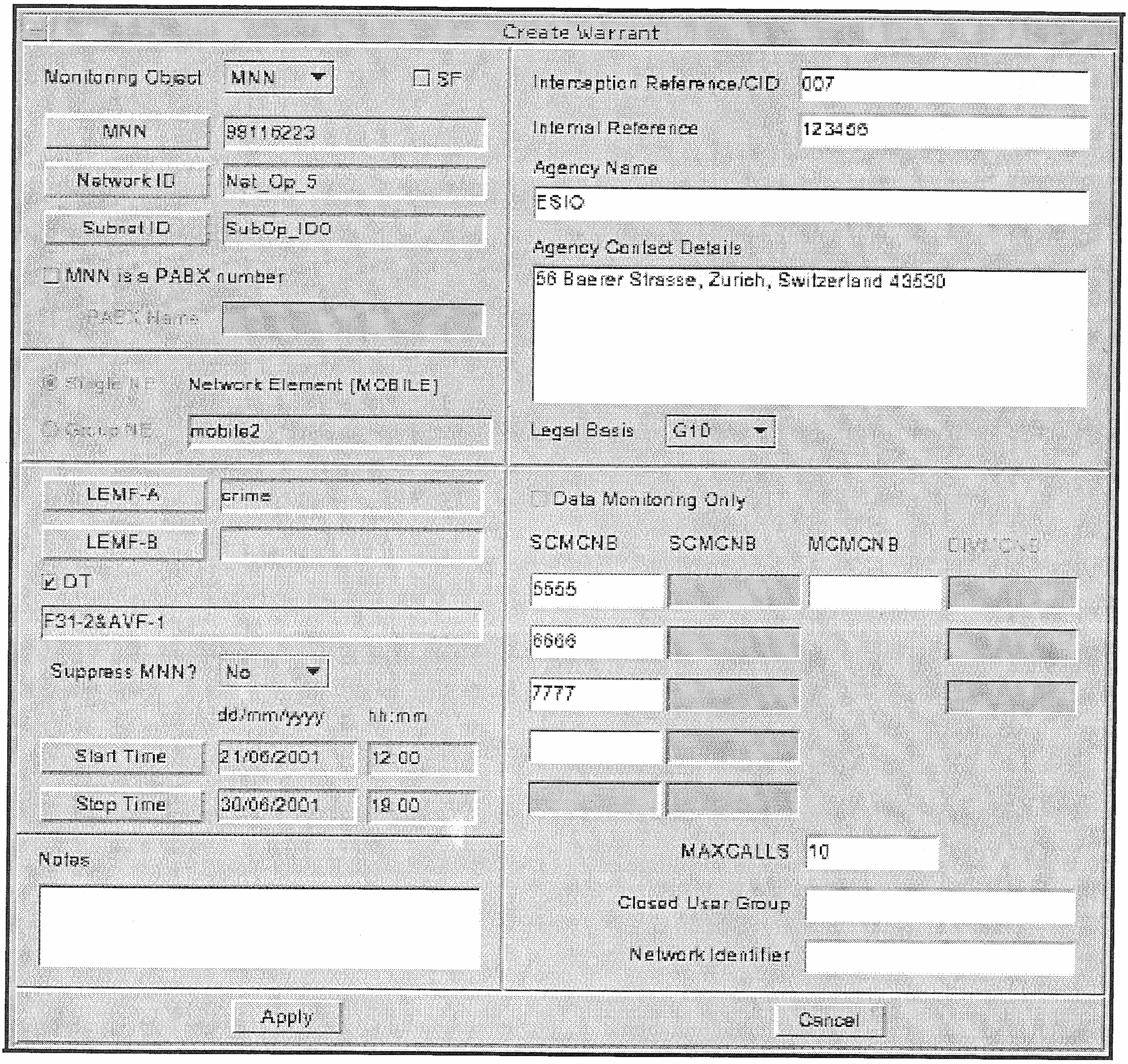



Διάφορα «παράθυρα» που εμφανίζονται στην οθόνη του χειριστή του Interceptions Management System.




Ίσως κάποιοι αναγνώστες, «πιο ψαγμένοι» περί τα τηλεφωνικά/ηλεκτρονικά , θα μπορέσουν να αντλήσουν περισσότερες και πιο ενδιαφέρουσες πληροφορίες. Αυτός είναι ο κύριος λόγος, για τον οποίο δημοσιεύουμε τόσες εικόνες, σχεδιαγράμματα, πληροφορίες τεχνικής φύσης.
Όποιος ενδιαφέρεται, μπορεί να περάσει μέρες ολόκληρες μπροστά σ' έναν υπολογιστή, ψάχνοντας τα σχετικά λήμματα σε «sites», όπως τα www.ericsson.com, www.wikipedia.org, www.google.gr, www.fas.org, www.statewatch.org, κ.λπ.




Ιδιαίτερο ενδιαφέρον παρουσιάζει το «παράθυρο διαλόγου» μέσω του οποίου ο χειριστής εισάγει στο σύστημα τα στοιχεία κάποιου «εντάλματος» κρατικής αρχής (αστυνομίας, υπηρεσίας πληροφοριών, δικαστηρίου, εισαγγελέα κ.λπ.), με το οποίο διατάσσεται η παρακολούθηση και καταγραφή των τηλεφωνικών επικοινωνιών κάποιου «υπόπτου» συνδρομητή και απαλλάσεται από κάθε ευθύνη ο «αρμόδιος υπάλληλος» που παραβιάζει το «συνταγματικά κατοχυρωμένο απόρρητο της ιδιωτικής ζωής» του ανυποψίαστου θύματος και των εξ ίσου ανυποψίαστων συνομιλητών του.

Γι' αυτούς τους τελευταίους, επισημαίνουμε ότι το «σύστημα» έχει την πρόσθετη ικανότητα να ΕΚΔΙΔΕΙ ΑΥΤΟΜΑΤΑ ΕΝΤΑΛΜΑΤΑ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ ΤΩΝ ΤΗΛΕΦΩΝΩΝ ΤΟΥΣ, εφ' όσον η σχέση τους με τον ύποπτο τούς καθιστά και αυτούς υπόπτους !!!

Τα υπόλοιπα κεφάλαια του «Εγχειριδίου» διαπραγματεύονται : το σύστημα ταξινόμησης και εύρεσης των αρχείων υποκλοπών (File Navigator - κεφ. 7), τις εντολές του συστήματος (IMS Commands - κεφ. 8), τους κωδικούς σφαλμάτων του συστήματος (IMS Alarm-Log - κεφ. 9), την «αναδρομολόγηση» της ροής των στοιχείων στην περίπτωση σφαλμάτων στην LEMF (LEMF Rerouting - κεφ. 10), την μορφή-format των αρχείων υποκλοπών (IMS Billing - κεφ. 11) και τα χαρακτηριστικά των «προϊόντων» του συστήματος (IMS Data-Products Specifications - κεφ. 12).
Το «Εγχειρίδιο» τελειώνει με «Γλωσσάρι», στο οποίο εξηγούνται τα χρησιμοποιούμενα αρχικά και οι διάφοροι όροι.

**Επιτρέψτε μας να κλείσουμε (για την ώρα) το θέμα με κάποιες δικές μας επισημάνσεις :**

- Η γραφή «centre», και όχι «center», προδίδει την βρεττανική παιδεία του συγγραφέα του «Εγχειριδίου».
- Όποιος αναγνώστης διαθέτει ηλεκτρονικό υπολογιστή και κινητό, θα έχει ακούσει τα παράσιτα που ακούγονται, λίγο πριν κουδουνίσει το δεύτερο από τα ηχεία του δευτέρου. Ένας καλύτερος δέκτης, σε συνδυασμό μ' έναν καλύτερο υπολογιστή μπορεί αυτόματα να μεταφράσει αυτό το σήμα σε αριθμούς που δείχνουν την ακριβή ραδιοσυχνότητα λήψης (ή εκπομπής) του κινητού τηλεφώνου. Ένας σχετικά ικανός τεχνίτης ραδιοφώνων μπορεί, εν συνεχεία, να «κλωνοποιήσει» το κινητό, δηλαδή να κατασκευάσει ένα ακριβές αντίγραφο, το οποίο θα κουδουνίζει όποτε κουδουνίζει και το πρωτότυπο, θα ακούει ό,τι ακούει κι εκείνο, θα δέχεται τα ίδια SMS και θα καταγράφει στη μνήμη του όσα καταγράφει και το αυθεντικό. Αυτού του είδους η υποκλοπή δεν είναι βέβαια «νόμιμη», κοστίζει όμως πολύ λιγότερο, δεν απαιτεί να γνωρίζουν πολλοί το μυστικό και, για τους λόγους αυτούς, οι διάφορες μυστικές υπηρεσίες προτιμούν αυτήν τη μέθοδο, τουλάχιστον, όταν το επιτρέπει η απόσταση απ' τον «στόχο» ή άλλες ειδικότερες συνθήκες και απαιτήσεις.
- Αν δεν βρίσκαμε το «Εγχειρίδιο» σε καμμιά δεκαριά διαδικτυακές «τοποθεσίες» κι αν δεν διασταυρώναμε κάποια στοιχεία του με όσα δημοσιεύονται στις επίσημες ιστοσελίδες της Ericsson, θα πιστεύαμε ότι είναι πλαστό. Το ότι, όμως, είναι γνήσιο δεν σημαίνει ότι δεν είναι και «φυτεμμένο», προκειμένου να παραπλανήσει και να καλύψει άλλες αλήθειες. Ο χρόνος, ωστόσο, της κυκλοφορίας του στο Internet αποκλείει την σχέση του με τις πολύ πιο πρόσφατες υποκλοπές στην Ελλάδα.
- Οι hackers κι όσοι ασχολούνται με την ασφάλεια των υπολογιστών και των δικτύων ξέρουν πολλούς και διάφορους τρόπους για να εγκαθιστούν σε κάποιο compiuter «παράνομο» λογισμικό ΕΞ ΑΠΟΣΤΑΣΕΩΣ. Πέρυσι μόλις, εντοπίστηκε πιτσιρικάς, ο οποίος με την χρήση του προγράμματος «RemotelyAnywhere» εισέδυσε σε περισσότερα από 100 δίκτυα του Πενταγώνου και άλλων κυβερνητικών υπηρεσιών των ΗΠΑ και από εκεί αντλούσε, επί κάμποσα χρόνια (!), «απόρρητα» στοιχεία, κυρίως οικονομικά, που τού επέτρεπαν να αρμέγει τους τραπεζικούς λογαριασμούς των στρατιωτικών. Εντοπίστηκε, τελικά, μόνο από την παρακολούθηση της κίνησης των τραπεζικών λογαριασμών στους οποίους κατέληγαν τα (κατά το νόμο) «κλοπιμαία». Με την χρήση, λοιπόν, κάποιου αντίστοιχου προγράμματος ή κάποιας έξυπνης τροποποίησης του «RemotelyAnywhere» (το οποίο μπορεί κανείς να βρεί και να «κατεβάσει» από το Internet), μπορεί κάποιος (πράκτορας, hacker ή απλά πλακατζής) να μπεί στο IMS, να υποκλέψει κωδικούς πρόσβασης που θα του επιτρέπουν να διαβάζει αρχεία, να κρυφακούει, να παρακολουθεί κι ακόμη να εγκαταστήσει κάποιο απλό λογισμικό που να εξαφανίζει κάθε ίχνος της εισβολής του...
- Έτσι, μόνο, από τις ταυτότητες των θυμάτων μπορεί κανείς να προσδιορίσει την ταυτότητα των δραστών των «ελληνικών υποκλοπών». Και μόνο με κλασσικές, αστυνομικές και κατασκοπικές μεθόδους μπορεί κανείς να τους παγιδεύσει (αν, βέβαια, το θέλει).
- Σίγουρη, λοιπόν, για την ουσιαστική αδυναμία απόδειξης της ενοχής της - και της ενοχής της Ericsson - η Vodafone εντείνει την διαφημιστική της καμπάνια στα ελληνικά ΜΜΕ, συνεχίζει ατάραχη να χειρίζεται το IMS και προάγει τον Κορωνιά. Σίγουρος, ο τελευταίος ότι κανείς δεν μπορεί - και δεν θέλει - να αποδείξει την ενοχή του, καταθέτει άνετα σε κοινοβουλευτικές επιτροπές και ανεξάρτητες αρχές. Και, σίγουροι, οι δολοφόνοι του Τσαλικίδη παρακολουθούν και σπάνε πλάκα με τα τεκταινόμενα...
- Όσο για την πρεσβεία των ΗΠΑ... Να, κι αν δεν αποδειχθεί !... Να, κι αν αποδειχθεί, η ενοχή της ! Εδώ δεν ιδρώνει τ' αυτί της με τα κακουργήματα που διαπράττει κατά της ανθρωπότητας, θα ιδρώσει με τις πλακίτσες που σκαρώνει στην «κυβέρνηση» της Ελλάδας ;
- Επαναλαμβάνουμε : ΤΟ IMS ΤΗΣ ERICSSON ΧΡΗΣΙΜΟΠΟΙΕΙΤΑΙ ΑΠ' ΟΛΕΣ ΤΙΣ ΕΤΑΙΡΙΕΣ ΣΤΑΘΕΡΗΣ ΚΑΙ ΚΙΝΗΤΗΣ ΤΗΛΕΦΩΝΙΑΣ ΤΗΣ ΧΩΡΑΣ.
- Να δείτε που όλα θα τελειώσουν με την πληρωμή - για καθαρά «λόγους τάξεως» και «γοήτρου» - με την καταβολή κάποιου ασήμαντου προστίμου...
- ΟΙ ΥΠΟΚΛΟΠΕΣ ΣΤΗΝ ΚΙΝΗΤΗ ΤΗΛΕΦΩΝΙΑ ΕΙΝΑΙ ΠΟΛΥ ΕΥΚΟΛΩΤΕΡΕΣ ΚΑΙ ΦΘΗΝΟΤΕΡΕΣ ΑΠ' Ο,ΤΙ ΣΤΗΝ ΚΙΝΗΤΗ.
- **Κι αν δεν έχετε το κουράγιο - ή την δυνατότητα - ΝΑ ΤΟ ΣΠΑΣΕΤΕ ΤΟ ΡΗΜΑΔΙ, ας έχετε τουλάχιστον την ευφυΐα ΝΑ ΤΟΥ ΒΓΑΖΕΤΕ ΤΗΝ ΜΠΑΤΑΡΙΑ στις δύσκολες στιγμές...**